

Application Number 09/810,986
Responsive to Office Action mailed April 29, 2005

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

Claim 1 (Currently Amended): A method comprising:
generating a link failure information identifying a failed link within a computer network;
and
communicating an update message to routers within the a computer network in
accordance with a routing protocol, wherein the update message ~~request withdrawal of~~ specifies
one or more routes through the computer network that rely upon the failed link and requests
withdrawal of the specified routes, and wherein the update message further incorporates the link
failure information to identify the failed link.

Claims 2-3 (Canceled).

Claim 4 (Previously Presented): The method of claim 1 further comprising generating the
update message to conform to the Border Gateway Protocol (BGP).

Claim 5 (Previously Presented): The method of claim 1, wherein generating link failure
information includes generating data defining a time period for storing the link failure
information, the method further comprising automatically deleting the link failure information
upon expiration of the time period.

Claim 6 (Previously Presented): The method of claim 1, wherein generating link failure
information includes generating data defining a time period for using the link failure information
to control routing decisions, the method further comprising automatically routing packets as if
the failed link has been restored upon expiration of the time period.

Application Number 09/810,986
Responsive to Office Action mailed April 29, 2005

Claim 7 (Original): The method of claim 1 further comprising routing data packets according to a path vector routing algorithm using the link failure information.

Claim 8 (Original): The method of claim 7, wherein routing data packets comprises routing data packets according to the Border Gateway Protocol (BGP).

Claim 9 (Original): The method of claim 1 further comprising detecting the failure of the link within the computer network.

Claim 10 (Original): A method comprising:
receiving link failure information identifying a failed link within a computer network;
receiving a packet identifying a destination within the computer network; and
forwarding the packet according to a path vector routing protocol using the link failure information.

Claim 11 (Original): The method of claim 10, wherein forwarding the packet comprises routing the packet according to the Border Gateway Protocol (BGP).

Claim 12 (Original): The method of claim 10, wherein forwarding the packet comprises:
selecting a route based on a routing table, wherein the route defines a path to the destination; and
discarding the route when the path uses the failed link.

Claim 13 (Currently Amended): The method of claim 10,
wherein the link failure information defines a valid time period for the information, ~~the method further comprising and~~
wherein forwarding the packet comprises forwarding the packet according to the link failure information prior to the expiration of the valid time period.

Application Number 09/810,986
Responsive to Office Action mailed April 29, 2005

Claim 14 (Currently Amended): The method of claim 13, ~~and wherein forwarding the packet comprises forwarding the packet without using the link failure information after the expiration of the valid time period.~~

Claim 15 (Original): The method of claim 10 further comprising:
storing the link failure information for a storage time period; and
selectively forwarding additionally received copies of the link failure information based on the expiration of the storage time period.

Claim 16 (Original): The method of claim 10 further comprising:
authenticating the link failure information; and
routing the packet using the link failure information when the link failure information is authenticated.

Claim 17 (Previously Presented): The method of claim 16, wherein authenticating the link failure information comprises verifying that the link failure information originated from a neighboring router.

Claim 18 (Currently Amended): A computer-readable medium having data structures thereon comprising:
a first data structure to store an identifier for a failed link within a computer environment;
~~and~~
a second data structure to store a unique identifier for an originator of the link failure information associated with the failed link, wherein the first data structure and the second data structure are stored within a routing table and associated in a manner that causes a network router to output a routing communication to withdraw one or more routes and specify the failed link identified within the first data structure ~~and without sending the routing communication; and~~
a third data structure to store a valid time period for the link failure information, wherein the third data structure causes the network router to route a packet according to the link failure

Application Number 09/810,986
Responsive to Office Action mailed April 29, 2005

information prior to expiration of the valid time period and route the packet without using the link failure information after the expiration of the valid time period.

Claim 19 (Cancelled).

Claim 20 (Currently Amended): The computer-readable medium of claim ~~18~~¹⁹, wherein the third data structure stores a pair of Internet Protocol (IP) addresses.

Claim 21 (Currently Amended): The computer-readable medium of claim 18, further comprising a ~~third~~ fourth data structure to store data defining a storage time for the link failure information.

Claim 22 (Currently Amended): The computer-readable medium of claim 18 further comprising:

- a ~~fourth~~ third-data structure to store a timestamp indicating when the link failed; and
- a ~~fifth~~ fourth-data structure to store security data for authenticating the originator.

Claim 23 (Currently Amended): A computer-readable medium containing instructions to cause a programmable processor to:

receive link failure information identifying a failed link within a computer network,
wherein the link failure information defines a valid time period for the information;

store the link failure information; and

forward a data packet to neighboring routers within the computer network according to the link failure information and a path vector routing protocol prior to expiration of the time period; and

forward packets as if the failed link has been restored upon expiration of the time period.

Claim 24 (Original): The computer-readable medium of claim 23 having instructions to cause the programmable processor to select a route for the data packet based on a routing table.

Application Number 09/810,986
Responsive to Office Action mailed April 29, 2005

Claim 25 (Cancelled).

Claim 26 (Original): The computer-readable medium of claim 23, wherein the path vector routing protocol comprises the Border Gateway Protocol (BGP).

Claim 27 (Currently Amended): A system comprising:
a data store to hold link failure information identifying a failed links within a computer network;
a routing table to store routing information describing available routes to nodes within the computer network; and
a control unit to forward packets through the computer network based on the link failure information and the routing information, wherein the control unit forwards the packets as if the failed link has been restored upon expiration of a valid time period associated with the link failure information.

Claim 28 (Original): The system of claim 27, wherein the control unit routes packets according to a path vector routing protocol.

Claim 29 (Original): The system of claim 28, wherein the path vector routing protocol comprises the Border Gateway Protocol (BGP).

Claim 30 (Original): The system of claim 27, wherein the control unit selects routes based on the routing table in order to route the packets around the failed links identified by the link failure information within the data store.

Claim 31 (Currently Amended): The system of claim 27, wherein the link failure information comprises data defining the a-valid time period for the link failure information.

Claim 32 (Original): The system of claim 27, wherein the link failure information comprises data defining a storage time period for the link failure information.

Application Number 09/810,986
Responsive to Office Action mailed April 29, 2005

Claim 33 (Original): The system of claim 27, wherein the link failure information comprises data defining a timestamp indicating when the link failed.

Claim 34 (Original): The system of claim 27, wherein the link failure information comprises data defining a unique identifier for an originator of the link failure information.

Claim 35 (Original): The system of claim 34, wherein the link failure information comprises security data for authenticating the originator.

Claim 36 (Original): The system of claim 34, wherein the control unit stores link failure information within the data store when the originator comprises a neighboring router.

Claim 37 (Previously Presented): The system of claim 27, wherein the data store comprises a routing table.

Claim 38 (Previously Presented): The system of claim 27, wherein the data store comprises a database.

Claim 39 (Currently Amended): A method comprising:
receiving a message including link failure information identifying a failed link within a computer network, wherein the link failure information defines a storage time period for which the link failure information is to be stored by a receiving router;
storing the link failure information within ~~a~~the router in accordance with the storage time period; and
selectively forwarding subsequently received messages that include the link failure information based on the expiration of the storage time period.

Application Number 09/810,986
Responsive to Office Action mailed April 29, 2005

Claim 40 (Previously Presented): The method of claim 39, wherein selectively forwarding comprises:

receiving a second message with the link failure message identifying the failed link; and
forwarding the second message only if the storage time period for the link failure message has expired.

Claim 41 (Previously Presented): The method of claim 39, further comprising automatically deleting the link failure information upon expiration of the storage time period.

Claim 42 (Previously Presented): A method comprising:

receiving a message including link failure information identifying a failed link within a computer network, wherein the message includes an origin identifier that identifies an originating network device that detected the link failure and a timestamp indicating when the failed link was detected;

accessing a data store to determine whether link failure information identifying the failed link, the originating network device and the timestamp has previously been received; and

forwarding the message only when the link failure information has not been previously received.

Claim 43 (Previously Presented): The method of claim 42,

wherein the message identifies at least one route having at least three nodes including a source node, a destination node and at least one intermediate nodes, and

wherein the failed link comprises a link coupling two of the nodes along the route.

Application Number 09/810,986
Responsive to Office Action mailed April 29, 2005

Claim 44 (Previously Presented): A method comprising:

receiving link failure information identifying a failed link within a computer network,
wherein the link failure information defines a valid time period for the link failure information;

receiving a packet identifying a destination within the computer network;

forwarding the packet according to a path vector routing protocol using the link failure
information prior to the expiration of the valid time period; and

forwarding the packet without using the link failure information after the expiration of the
valid time period.